The Third SHA-3 Candidate Conference

March 22-23, 2012
Washington Marriott Hotel, Washington, DC USA
West End Ballroom CDE

Program

First Day ***Thursday, March 22, 2012***	
7:30 am	**Registration Opens**
9:00 – 9:15 (15 minutes)	**Opening Remarks** Donna Dodson, Chief, Computer Security Division, *NIST*
9:15 – 10:40 (85 minutes)	**Session I: Security Analysis I** (20 minutes each) **Session Chair:** Morris Dworkin, *NIST* 1. **A Study of Practical-time Distinguishing Attacks Against Round-reduced Threefish-256** *Presented by:* Aron Gohr, Bundesamt für Sicherheit in der Informationstechnik (BSI) 2. **ARXtools: A Toolkit for ARX Analysis** *Presented by:* Pierre-Alain Fouque, ENS 3. **On the Algebraic Degree of some SHA-3 Candidates** *Presented by:* Christina Boura, INRIA/Gemalto 4. **Side Channel Analysis of the SHA-3 Finalists** *Presented by:* Michael Zohner, CASED
10:40 – 11:05 (25 minutes)	**Coffee Break**
11:05 – 12:30 (85 minutes)	**Session II: Security Analysis II** (20 minutes each) **Session Chair:** Rene Peralta, *NIST* 1. **Provable Security of BLAKE with Non-Ideal Compression Function** *Presented by:* Bart Mennink, KULeuven 2. **Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Groestl, JH, Keccak, and Skein** *Presented by:* Elena Andreeva, KULeuven 3. **Improved Indifferentiability Security Bound for the JH Mode** *Presented by:* Souradyuti Paul, NIST and KULeuven 4. **A Keyed Sponge Construction with Pseudorandomness in a Standard Model** *Presented by:* Donghoon Chang, NIST

Thursday, March 22, 2012	
12:30 – 13:45 (75 minutes)	**Lunch** *Room: Dupont Salon FG*
13:45 – 14:50 (65 minutes)	**Session III: Hardware Implementations I** (20 minutes each) **Session Chair:** Bill Burr, *NIST* 1. **Lessons Learned from Designing a 65nm ASIC for Evaluating Third Round SHA-3 Candidates** *Presented by:* Frank Gurkaynak, Microelectronics Design Center, ETH Zurich, Switzerland 2. **Comprehensive Evaluation of High-Speed and Medium-Speed Implementations of Five SHA-3 Finalists Using Xilinx and Altera FPGAs** *Presented by:* Kris Gaj, George Mason University 3. **Efficient Hardware Implementations and Hardware Performance Evaluation of SHA-3 Finalists** *Presented by:* Athar Mahboob, National University of Sciences and Technology, Islamabad, Pakistan
14:50 – 15:15 (25 minutes)	**Coffee Break**
15:15 – 16:20 (65 minutes)	**Session IV: Hardware Implementations II** (20 minutes each) **Session Chair:** Andy Regenscheid, *NIST* 1. **On the Suitability of SHA-3 Finalists for Lightweight Applications** *Presented by:* Elif Bilge Kavun, Horst Görtz Institute, Ruhr University - Bochum 2. **Lightweight Implementations of SHA-3 Finalists on FPGAs** *Presented by:* Jens-Peter Kaps, George Mason University 3. **Evaluation Of Compact FPGA Implementations For All SHA-3 Finalists** *Presented by:* Bernhard Jungk, University of Applied Sciences Wiesbaden

<table>
<tr><th colspan="2"><i>Thursday, March 22, 2012</i></th></tr>
<tr><td><b>16:20 – 17:10</b>
(50 minutes)</td><td><b>Session V: Algorithm Specific Implementations</b> (15 minutes each)
<b>Session Chair:</b> Meltem Sonmez Turan, <i>NIST</i>

1. <b>BLAKE and 256-bit advanced vector extensions</b>
<i>Presented by:</i> Samuel Neves, Universidade de Coimbra
2. <b>Grøstl Implementation Guide</b>
<i>Presented by:</i> Martin Schläffer, IAIK, Graz University of Technology
3. <b>1001 ways to implement Keccak</b>
<i>Presented by:</i> Guido Bertoni, STMicroelectronics</td></tr>
<tr><td><b>17:10</b></td><td><b>Adjourn for Day</b></td></tr>
</table>

<table>
<tr><th colspan="2"><i>Second Day</i>
<i>Friday, March 23, 2012</i></th></tr>
<tr><td><b>8:00 am</b></td><td><b>Registration Opens</b></td></tr>
<tr><td><b>9:00 – 10:25</b>
(85 minutes)</td><td><b>Session VI: Software Implementations</b> (20 minutes each)
<b>Session Chair:</b> Larry Bassham, <i>NIST</i>

1. <b>The New SHA-3 Software Shootout</b>
<i>Presented by:</i> Dan Bernstein, University of Illinois and Tanja Lange, Technische Universiteit Eindhoven
2. <b>XBX Benchmarking Results January 2012</b>
<i>Presented by:</i> Christian Wenzel-Benner, ITK Engineering AG
3. <b>SHA-3 on ARM11 Processors</b>
<i>Presented by:</i> Bo-Yin Yang, Academia Sinica, Taiwan
4. <b>Performance of the SHA-3 Candidates in Java</b>
<i>Presented by:</i> Christian Hanser, Institute for Applied Information Processing and Communications, Graz University of Technology</td></tr>
<tr><td><b>10:25 – 10:50</b>
(25 minutes)</td><td><b>Coffee Break</b></td></tr>
<tr><td><b>10:50 – 12:05</b>
(75 minutes)</td><td><b>Session VII: Open Discussion I - Performance</b>
<b>Session Chair:</b> Bill Burr, <i>NIST</i>

*Please see discussion questions at end of program</td></tr>
<tr><td><b>12:05 – 13:20</b>
(75 minutes)</td><td><b>Lunch</b>
<i>Room : Dupont Salon FG</i></td></tr>
</table>

Friday, March 23, 2012	
13:20 – 15:05 (105 minutes)	**Session VIII: Round 3 Candidates Presentation** (20 minutes each) **Session Chair:** Lily Chen, *NIST* 1. **BLAKE** *Presented by:* Jean-Philippe Aumasson, Nagravision SA 2. **Grøstl** *Presented by:* Christian Rechberger, DTU 3. **JH** *Presented by:* Honjun Wu, Institute for Infocomm Research 4. **Keccak** *Presented by:* Gilles Van Assche, STMicroelectronics 5. **Skein** *Presented by:* Bruce Schneier, BT
15:05 – 15:30 (25 minutes)	**Coffee Break**
15:30 – 16:55 (85 minutes)	**Session IX: Open Discussion II** **Session Chair:** John Kelsey, *NIST* 1. **Batteries Included- Features and Modes for Next Generation Hash Functions** (20 minutes) *Presented by:* Stefan Lucks, Bauhaus-Universität Weimar 2. **Open Discussion** *Please see discussion questions at end of program
16:55 – 17:10 (15 minutes)	**Closing Remarks** Bill Burr, *NIST*
17:10	**Adjourn**

The Third SHA-3 Candidate Conference Open Discussion Questions

Session VII: Open Discussion I - Performance

1) What algorithms give us the best coverage in places where SHA-256 and SHA-512 perform badly? Where does SHA-2 performance seem weakest?
   a) Should we think about this in our selection?

2) NIST is interested in figuring out what performance differences among SHA-3 finalists will have a practical impact on real-world applications, specifically whether there are current or near-future applications where these differences will determine whether the application can use SHA-3 or not. Identify specific applications and candidate algorithm that are unlikely to use SHA-3 if that candidate is chosen to be SHA-3.

3) Should parallelizability matter in our selection, assuming that we will produce a tree-mode hashing document sometime after the SHA-3 competition completes?

4) What performance issues haven't we considered in this conference that we should consider?

5) How much weight should we give to 512-bit hash versions vs. 256-bit hash versions?
   a) Are there some SHA-3 versions where the 512 bit hash is generally a better performer, and should be compared with the 256-bit versions of other candidates?

6) Dividing the world into unconstrained and constrained implementations and into hardware and software implementations:
   a) Which quadrant is the most important? Which is the least important?
   b) What criteria would you use to define a "constrained" implementation?
   c) Where does an ARM with the NEON SIMD instructions fall on the above scale?
   d) Can you assign a weight to each of these categories for performance ranking purpose, and explain why?
   e) Which finalist seems to have the best performance in each of the categories mentioned above, and in overall performance?
   f) We don't seem to have many implementations that took advantage of the NEON SIMD extension. Is it fair to assume that such extension will boost the performance of all (or at least most) SHA-3 finalists? If not, why not?
   g) It seems that adding 64-bit rotations to vector instruction sets might speed up Skein, Keccak and BLAKE. Is that so? Are there other simple extensions to vector instruction sets that might speed up particular candidates?
   h) Mbits/Joule seems a natural metric for measuring power consumption, but we don't have much power consumption data. Throughput seems a reasonable power consumption proxy for software. Is throughput/area a reasonable proxy for hardware?

7) What new and upcoming applications and environments could use SHA-3 without having to transition from SHA-1 or SHA-2? In these cases, there would be no transition required.

Session IX: Open Discussion II

Security

1) Do any of the published analyses give much insight into which algorithm is more likely to fall to a real attack (academic or practical) in its lifetime?
   a) What are the most damaging or worrisome attacks to each of the SHA-3 finalists so far?
   b) Are there any results on these candidates that, right now, should call them into question?
   c) If so, what are they, and how can we better understand what we should learn from these results?

2) How important is side channel resistance in hashing applications?
   a) Are there important differences in candidates' resistance to side channel attacks, or ease of securing them against side-channel attacks?
      i) Groestl and S-boxes?
      ii) Skein/BLAKE and additions?

3) Which candidate would you say is the best understood, in security terms, at this point?
   a) Are there candidates you think are still poorly understood in security terms?
   b) Are some candidates' designs inherently harder to understand well in that sense than others?

SHA-3 Selection

1) Should we try to find a SHA-3 candidate with a large design difference from SHA-2 or from AES?
2) Should we care about "extras" like the Keccak authenticated encryption mode or the Threefish wide tweakable block cipher?
3) Individual SHA-3 Designers: If you couldn't pick your candidate, which one would you pick?
4) Non-Designer, Non-NIST Audience: Which candidate would you pick, if it were your decision?
5) Everyone: Are there any candidates that you think explicitly should not be picked? If so, why?